Remarks

The present Amendment and Response is believed to be fully responsive to the Final Office Action dated July 17, 2008. The Amendment and Response is submitted concurrently with a Request for Continued Examination (RCE) and the appropriate fee. After entry of the present Amendment, Claims 12-39 remain pending. By this Amendment, independent Claims 12 and 21 and have been amended. New dependent Claims 38 and 39 have been added. Claims 1-11 were previously withdrawn by prior response. It is respectfully submitted that no new matter has been added by the foregoing amendments. Reconsideration of the application is requested in view of the following remarks.

Claim Rejections Under 35 U.S.C. § 103

In the Final Office Action, Claims 12, 14-17, 21, 23-26, and 30-39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,422,953 to Fischer (hereinafter "*Fischer*") in view of U.S. Pat. No. 6,049,874 to McClain et al. (hereinafter "*McClain*") and further in view of U.S. Pat. No. 6,990,588 to Yasukura (hereinafter "*Yasukura*"). Claims 13 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of *McClain* and *Yasukura* and further in view of U.S. Pat. No. 6,775,772 to Binding et al. (hereinafter "*Binding*"). Claims 18 and 27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of *McClain* and *Yasukura* and further in view of the Applicant's allegedly Admitted Prior Art (hereinafter "AAPA"). Claims 19, 20, 28, and 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of *Fischer*, *McClain*, *Yasukura*, and the AAPA in view of U.S. Pat. No. 6,594,759 to Wang (hereinafter "*Wang*").

By the present Amendment, independent Claims 12 and 21 have been amended in order to clarify the scope of the claimed invention of Claims 12 and 21. Specifically, independent Claim 12 has been amended to include "generating, within the secure device, a verification status indicator based at least in part on a comparison of pre-stored verification data stored by the

secure device to input verification data received from a user of the secure device, wherein the verification status indicator does not include the pre-stored verification data or the input verification data" (Underlining supplied). Independent Claim 21 has been amended in a similar manner. Support for these amendments is provided at least in paragraphs [0133] – [0137] of the Specification as published and also in Figure 5 at element 514. For example, paragraphs [0134] and [0135] state in part:

> **[0134]** The device **240** also includes a set of predefined verification statuses each representing a relational correspondence between the verification data **250** and the prestored data **270** ... The indicator **260** output from the device **240** is based on the last comparison of the verification data **250** with the prestored data **270**, but only if input representing verification data **250** has been received since the resetting of the device. Otherwise, the indicator **260** indicates the lack of input representing verification data **250** since the resetting of the device **240**. In either case, the indicator **260** is transmitted in association with the EC **210**, whereby the recipient is able to identify the indicator **260** as relating to the EC **210** ...
>
> **[0135]** ... None of the verification statuses actually reveal the verification data **250** or the prestored data **270**; thus, no "shared secret" is required between the sender **220** and the recipient. However, the recipient can infer correct knowledge of the Secret from the verification status.

In marked contrast to the claimed invention, neither *Fischer*, *McClain*, *Yasukura*, *Binding*, nor *Wang*, either taken alone or in combination, disclose, teach, or suggest generating a

verification status indicator within the secure device, wherein the verification status indicator does not include the pre-stored verification data or the input verification data and providing the verification status indicator to the computer program application, as recited by the amended independent claims. Although *Fischer* discusses the certification of a user of a personal data/time notary device, the certification is conducted by a certifier and not by the device itself (See *Fischer* at column 6, lines 43-57). There is no teaching or suggestion of a validation of a user being conducted by the device by comparing pre-stored verification data stored by the device to input verification data received from a user of the device. Additionally, there is no teaching or suggestion of generating a verification status indicator within the device that does not include the pre-stored verification data or the input verification data. In fact, the Office Action recognizes on page 3 that *Fisher* fails to teach these features. Accordingly, it is respectfully submitted that *Fischer* does not teach or suggest generating a verification status indicator within the secure device and providing the verification status indicator to a computer program application with a generated digital signature, as recited by the amended independent claims.

The Office Action relies on *Yasukura* to teach the feature of including an authentication result (i.e., verification status indicator) with a transaction. *Yasukura*, however, does not teach or suggest generating, within the secure device, a verification status indicator based at least in part on a comparison of pre-stored verification data stored by the secure device to input verification data received from a user of the secure device, wherein the verification status indicator does not include the pre-stored verification data or the input verification data. In *Yasukura*, the authentication of a user is performed at an authentication access terminal that obtains biological data of a user (See *Yasukura* at Col. 4, lines 14-17). A portion of the obtained biological data is compared to biological data that is stored on an authentication card carried by a user, and another portion of the obtained biological data is communicated to a certification authority for comparison to biological data stored at the certification authority (See *Yasukura* at Col. 4, lines 14-23). If the authentication card carried by the user is found to be the secure device recited in the claims, then no generation of a verification status indicator is made within the secure device.

On the other hand, if the authentication access terminal is found to be the secure device, then no comparison is made within the secure device between input verification data and pre-stored verification data stored by the secure device.

Assuming, arguendo, that *Yasukura* is found to disclose generating, within the secure device, a verification status indicator based at least in part on a comparison of pre-stored verification data stored by the secure device to input verification data received from a user of the secure device, there is still no teaching or suggestion in *Yasukura* of generating a verification status indicator that does not include the pre-stored verification data or the input verification data, as recited by the amended independent claims. As set forth in the Background of the present application, potential security risks exist when Secrets or biometric values utilized in Factor B Entity Authentication and Factor C Entity Authentication are shared or communicated (See Specification at paragraphs [0013] - [0016]). Therefore, the authentication performed in *Yasukura* includes security risks because biological data (e.g., biometric values) is shared with multiple parties, including an authentication access terminal and a certification authority (See *Yasukura* at Col. 4, lines 14-22). Such a system does not provide the same level of security as that of various embodiments of the claimed invention, in which a verification is conducted within a secure device and in which Secrets and/or biometric data are not communicated outside of the secure device. Accordingly, it is respectfully submitted that *Yasukura* does not teach or suggest each and every element of the amended independent claims.

Furthermore, *McClain*, *Binding*, and *Wang* all fail to teach or suggest the feature of generating a verification status indicator within the secure device and providing the verification status indicator to the computer program application. *McClain*, *Binding*, and *Wang* also fail to teach or suggest that the generating verification status indicator does not include the pre-stored verification data or the input verification data.

As a result of providing the verification status indicator to the computer program application, the computer program application or another component or system in communication with the computer program application may determine a verification status of the

secure device based on the verification status indicator (See, for example, Specification at paragraph [0149]). A level of risk associated with the message data may be determined based on the verification status (*See, for example*, Specification at paragraph [0128]. Additionally, the verification status of the device may be determined without revealing a shared secret of the device, such as a user's PIN or biometric data associated with the user (See, for example, Specification at paragraphs [0137]). Accordingly, additional security may be provided to a recipient without compromising sensitive data of a user. For at least these reasons, it is respectfully asserted that amended independent Claims 12 and 21 are allowable over *Fischer*, *McClain*, *Yasukua*, *Binding*, and *Wang*, either taken alone or in combination. Therefore, it is respectfully contended that the amended independent claims are in condition for allowance.

Additionally, it is respectfully submitted that dependent Claims 13-20 and 22-37 are allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features. Accordingly, it is respectfully asserted that the pending claims of the application are in condition for allowance and prompt allowance of the same is requested.

Patentability of Dependent Claims 38 and 39

New dependent Claims 38 and 39 were added by the Amendment and Response filed on April 23, 2008. Dependent Claim 38 includes the recitation of the message data being "modified by the verification status indicator prior to originating the digital signature." Additionally, dependent Claim 38 includes the recitation of the verification status indicator to being provided to the computer program as "a component of the generated digital signature." Dependent Claim 39 includes similar recitations. Support for these claims is provided at least in paragraph [0225] of the Specification.

Although the Office Action indicates that these claims are unpatentable over *Fischer* in view of *McClain* and *Yasukura*, the Office Action offers no explanation for these rejections. It is respectfully submitted that neither *Fischer*, *McClain*, *Yasukura*, *Binding*, nor *Wang*, either taken

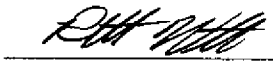
alone or in combination, teaches or suggests modifying the message data with a verification status indicator prior to originating the digital signature, such that the verification status indicator is included in the digital signature. Accordingly, it is respectfully submitted that dependent Claims 38 and 39 recite features that are not taught or suggested by the cited art of record. Additionally, it is respectfully asserted that dependent Claims 38 and 39 are allowable as a matter of law as depending from an allowable base claim for which arguments for patentability are set forth above. For at least these reasons, it is respectfully contended that dependent Claims 38 and 39 are allowable over the cited art of record.

Conclusion

It is believed that each matter raised by the Final Office Action has been addressed. It is not believed that extensions of time or fees for net addition of claims are required beyond those which may be otherwise provided for in the documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 19-5029.

If there are any issues which can be resolved by teleconference call or an Examiner's Amendment, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



Rhett S. White
Reg. No. 59,158

Date: **October 17, 2008**

SUTHERLAND ASBILL & BRENNAN LLP
999 Peachtree Street, NE
Atlanta, Georgia 30309-3996
Telephone: 404.853.8037
Facsimile: 404.853.8806

FDC No. 019500US

Attorney Docket: 34250-1174